

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-325224

(P2001-325224A)

(43) 公開日 平成13年11月22日 (2001. 11. 22)

(51) Int.Cl.<sup>7</sup>

G 0 6 F 15/00

識別記号

3 3 0

F I

G 0 6 F 15/00

テーマコード\*(参考)

3 3 0 A 5 B 0 8 5

審査請求 未請求 請求項の数 3 O L (全 7 頁)

(21) 出願番号 特願2000-142970(P2000-142970)

(22) 出願日 平成12年 5 月16日 (2000. 5. 16)

(71) 出願人 399117110

日本ヒューレット・パッカード株式会社

東京都杉並区高井戸東 3 丁目29番21号

(72) 発明者 小早川 直樹

東京都杉並区高井戸東 3 丁目29番21号 日

本ヒューレット・パッカード株式会社内

(74) 代理人 100081721

弁理士 岡田 次生 (外 1 名)

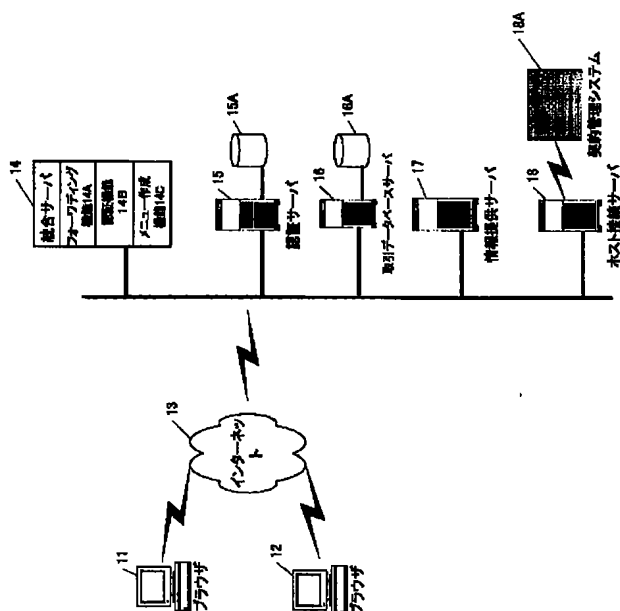
F ターム(参考) 5B085 AA08 AE00 AE23 CE03 CE04

(54) 【発明の名称】 通信システム

(57) 【要約】

【課題】 ユーザが自己のアクセス権限の範囲を心配することなくメニューにしたがってウェブページをアクセスすることができるシステムを提供する。

【解決手段】 この発明の通信システムは、複数のウェブサーバとブラウザとの間の通信を制御する統合サーバと、前記複数のウェブサーバが備えるファイルの少なくとも 1 つにアクセスする権限を有するユーザの識別情報およびアクセス権限情報を有する認証サーバと、を備え、統合サーバは、ユーザからのアクセス要求に応じて、認証サーバと通信しユーザのアクセス権限を確認し、アクセス権限に対応する項目を含んだメニューページを作成してユーザに返すダイナミック・メニュー作成機能を有する。一つの形態において、ダイナミック・メニューを作成するための HTML 文書であるテンプレートを備え、該テンプレートは、ユーザの属性に応じたページへのハイパーリンクの記述を含んでいる。



## 1

## 【特許請求の範囲】

【請求項1】複数のウェブサーバとブラウザとの間の通信を制御する統合サーバと、前記複数のウェブサーバが備えるファイルの少なくとも1つにアクセスする権限を有するユーザの識別情報およびアクセス権限情報を有する認証サーバと、を備え、前記統合サーバは、ユーザからのアクセス要求に応じて、前記認証サーバと通信し該ユーザの前記アクセス権限を確認し、該アクセス権限に対応する項目を含んだメニューページを作成してユーザに返すダイナミック・メニュー作成機能を有する通信システム。

【請求項2】前記ダイナミック・メニューを作成するためのHTML文書であるテンプレートを備え、該テンプレートは、ユーザの属性に応じたページへのハイパーリンクの記述を含んでいる請求項1に記載の通信システム。

【請求項3】ユーザの属性グループごとに用意された複数のページのURLを含む設定ファイルを備え、前記ハイパーリンクの記述は、前記属性グループに関する変数を含んでおり、前記ダイナミック・メニュー作成の際、アクセス中のユーザの前記属性グループに対応するURLが該変数に代入されるよう構成した請求項2に記載の通信システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】この発明は、ネットワーク・システムにおけるユーザ認証およびダイナミック・メニューの作成に関する。

## 【0002】

【従来の技術】一般にネットワーク・システムにおいて、ユーザの認証はサーバ単位で実現している。業務上複数のサーバを設ける場合、ユーザ登録およびアクセス権限の設定はサーバごとに行なう。この方式では、ユーザの立場から、自己がどのサーバについてどういうアクセス権限を持っているかが判然とせず、実際にユーザIDおよびパスワードを入力してアクセスを試みて、アクセスを拒否されて自己にアクセス権限がないことを知ることがあった。さらに、それぞれのサーバ単位でユーザIDおよびパスワードの入力を要求され使い勝手が悪いという問題があった。

【0003】特開平10-269184号公報には、証明証を利用して統合認証サーバがDBサーバおよび業務サーバに対するユーザのアクセス権限をチェックする方式が記載されている。

【0004】また、特開平11-25048号公報には、統合認証サーバがクライアントから送られてくる統合証明書に関してアクセス権限をチェックし、正当であれば、通信当事者に証明書を送付し、通信を確立することが記載されている。

## 【0005】

【発明が解決しようとする課題】これらの公開公報に記

## 2

載される技術は、複数のサーバに対するユーザの認証を統合するものではあっても、ユーザのアクセス権限の一覧をユーザに提示するものではないから、複雑にアクセス権限が設定されている場合、ユーザは自己にどの範囲のアクセス権限が設定されているかについて記憶しておくなり、アクセスの度にメモを参照する必要があるという問題を含んでいる。

## 【0006】

【課題を解決するための手段】上記の課題を解決するため、この発明の通信システムは、複数のウェブサーバとブラウザとの間の通信を制御する統合サーバと、前記複数のウェブサーバが備えるファイルの少なくとも1つにアクセスする権限を有するユーザの識別情報およびアクセス権限情報を有する認証サーバと、を備え、統合サーバは、ユーザからのアクセス要求に応じて、認証サーバと通信しユーザのアクセス権限を確認し、アクセス権限に対応する項目を含んだメニューページを作成してユーザに返すダイナミック・メニュー作成機能を有する。

【0007】このようにすることにより、ユーザには、ユーザのアクセス権限に応じたメニューページが提示されるので、ユーザは、自己のアクセス権限の範囲を心配することなく、メニューにしたがってウェブページにアクセスすることができる。

【0008】この発明のシステムは、一つの形態において、ダイナミック・メニューを作成するためのHTML文書であるテンプレートを備え、該テンプレートは、ユーザの属性に応じたページへのハイパーリンクの記述を含んでいる。

【0009】さらに具体的な形態において、この発明のシステムは、ユーザの属性グループごとに用意された複数のページのURLを含む設定ファイルを備え、ハイパーリンクの記述は、属性グループに関する変数を含んでおり、ダイナミック・メニュー作成の際、アクセス中のユーザの属性グループに対応するページのURLがこの変数に代入される。

## 【0010】

【発明の実施の形態】次に図面を参照してこの発明の実施の形態を説明する。図1は、この発明の一実施形態のコンピュータ・ネットワークの全体的な構成を示すブロック図である。

【0011】ブラウザ11、12は、典型的にはパーソナル・コンピュータに組み込まれた閲覧ソフトウェア、たとえばネットスケープ（商標）、インターネット・エクスプロアラ（商標）、によって実現され、インターネット13またはイントラネットを介してインターネット・プロトコルにより統合サーバ14に接続される。ブラウザと統合サーバ14との通信はSSL暗号機能を使用して行われる。

【0012】統合サーバ14は、ブラウザから送信される認証CookieまたはユーザIDおよびパスワードを認証サ

## 3

サーバ15に送り、ユーザのアクセス権限の認証を行う認証機能14Bを備えている。

【0013】ネットワークには複数のウェブサーバとして取引データベースサーバ16、情報提供サーバ17、およびホスト接続サーバ18が接続されている。たとえば保険業務での適用を例にとると、取引データベースサーバ16は代理店関連の取引データのデータベース16Aのためのウェブサーバである。情報提供サーバ17は、マニュアル、新商品などの情報を代理店および社員に提供するためのウェブサーバである。ホスト接続サーバ18は、契約管理システム18Aに接続するためのウェブサーバである。

#### 【0014】ダイナミック・メニューの構成

図2および図3を参照しながらダイナミック・メニューの構成を説明する。ダイナミックメニューは、たとえば図3に示す形態をとり、メニューページに埋め込まれてユーザのブラウザに表示される。この例ではNEW!新着情報のボタン42がダイナミックに作成されており、このボタンをクリックすると、アクセス中のユーザの属性グループに対応するページが表示される。ボタン43aから43eは、通常のハイパーリンクのボタンであり、ユーザの属性に関わらずそれぞれ同じウェブページにリンクされている。ボタン44は、パスワード変更手続きに入るためのもので、ボタン45は、ログアウトするためのボタンである。

【0015】図2において、統合サーバ14のフォワードイング機能14Aは、インターネット13を介してブラウザ11、12と通信を行う機能である。ブラウザ11からのアク

## 4

セスに対して認証サーバ15による認証がなされると、メニュー作成機能14CがHTML文書であるテンプレート32を読み出す。このテンプレートは、ボタン42を表示するために、たとえば改行タグ<BR>から始まる次に示す内容の記述を含んでいる。

#### 【0016】

```
<BR>
<TABLE BORDER=1 WIDTH=" 100%" >
<TR><TD ALIGN=" CENTER" BGCOLOR=" #DDDD" >
<FONT COLOR=" #FF000" ><STRONG>NEW! </STRONG><FONT
>
<A HREF=" $S_NEW" TARGET=" VIEW" >新着情報</A>
</TD></TR>
</TABLE>
```

【0017】この記述の中で、<Aおよび<A>は、アンカータグと呼ばれ、ハイパーリンクを規定するタグである。この例では、「新着情報」と表示されるボタンをクリックすると、\$S\_NEWが示すURLにページが飛ぶことを規定している。\$S\_NEWは、ユーザの属性に応じて設定ファイル31から読み出されて代入されるURLである。したがって、ユーザに送信されるメニューページにおいては、\$S\_NEWの箇所に具体的なURLが入れられている。

【0018】設定ファイル31は、たとえば次の表に示す内容を含んでいる。この例ではユーザの属性としてユーザの所属するグループをとっている。

#### 【0019】

【表1】

所属グループ	表示するページのURL
grp00	https://www.abc.co.jp/xyz/whatsnew1
grp01	https://www.abc.co.jp/xyz/whatsnew2
grp02	https://www.abc.co.jp/xyz/whatsnew3
grp03	https://www.abc.co.jp/xyz/whatsnew4
grp04	https://www/abc.co.jp/xyz/whatsnew5

【0020】ユーザからのアクセス要求があると、後にアクセス制御のセクションで説明するように、認証サーバ15のアクセス権限チェック機能15BがユーザIDまたはユーザの属性を記述する情報に基づいてユーザの所属グループを判断する。いまの場合、ユーザがgrp02に所属するとすると、統合サーバは、https://www.abc.co.jp/xyz/whatsnew3を表1の設定ファイルから読み出し、テンプレート32における上述のアンカー中の\$S\_NEWに代入する。こうして作成されたメニューページがブラウザ11に送られる。

【0021】こうしてブラウザ11に表示されたメニューページでは、新着情報のボタン42は、https://www.abc.co.jp/xyz/whatsnew3にハイパーリンクが形成されている。したがって、このボタンをクリックすると、whatsn

ew3のページがブラウザに表示される。こうしてユーザには、ユーザに適した項目だけのページが提示される。

#### 【0022】ユーザ認証

次に図4を参照してユーザ認証のプロセスを説明する。ブラウザ11がhttpプロトコルにしたがって統合サーバ14にアクセス要求を送ると(101)、統合サーバ14、より具体的には図1におけるフォワードイング機能14A、がこれを受信し、認証Cookieの有無をチェックする(102)。Cookie(クッキー)は、httpプロトコルで使われる小さいファイルであり、サーバ側のスクリプトから任意の情報を詰めてブラウザに送られる。この実施例における認証Cookieは、後に説明するように認証が成功したときブロック123で設定されてブラウザ11に送られるものである。

## 5

【0023】認証Cookieがないときは、統合サーバ14はログインページのhtmlファイルを読み出してブラウザに送る(104)。ユーザがブラウザ11に表示されるログインページにユーザIDおよびパスワードを入力して送信すると、統合サーバ14は、送られてきた情報を用いてユーザ認証メッセージを作成し、認証サーバ15に送る(106)。これに回答して認証サーバ15は、記憶装置15Aに格納されているユーザIDおよびユーザパスワードと送信されてきたユーザIDおよびユーザパスワードとの整合性をチェックし(107)、整合しなければ、NG応答メッセージを統合サーバ14に返す(108)。これを受けて統合サーバ14は、ログインエラーページを生成してブラウザ11に送る。NGの原因がパスワードの期限切れの場合は、統合サーバ14は、パスワード変更ページをブラウザ11に送る(109)。

【0024】ログインエラーページまたはパスワード変更ページは、ブラウザ11に表示され(110)、ユーザは再度ログインを試み、またはパスワードの変更手続きをすることができる。

【0025】ブロック107にもどり、ユーザ認証がOKの場合、認証サーバ15は、認証がOKであることを示すデータを入れた認証Cookieを作り(121)、OKメッセージとともに統合サーバ14に送る(122)。統合サーバ14は、認証Cookieを設定し、図5のアクセス制御プロセスに移るとともに、ブラウザ11に認証Cookieを送る(123)。ブラウザ11は、認証Cookieをそのユーザ固有の情報として保存し、次に統合サーバ14にアクセスするとき統合サーバ14に送信する。ブロック102にもどると、統合サーバ14は、ブラウザからのアクセス要求に認証Cookieがついていると、図5のアクセス制御プロセスに移る。

【0026】認証サーバは、統合サーバ14に接続したユーザのユーザIDを保持し、接続から切断までのサービス選択状況を監視し、その記録(ログ)をとる。また、

## 6

認証サーバ15は、無停止を前提として構成されており、システムの稼働中に新規ユーザの登録や既存のユーザの削除を実行することができる。

## 【0027】アクセス制御

統合サーバ14は、アクセス要求メッセージを認証サーバ15に送る(204)。これを受けて認証サーバ15は、認証Cookieのチェックを行い、有効であればこのユーザが要求中のファイルへのアクセス権限をもつかどうかをアクセス権限テーブルを参照してチェックする(206)。このユーザがアクセス権限を持っていることが確認されると、認証サーバ15は、OKメッセージを統合サーバ14に送る(207)。アクセス権限テーブルは、たとえば次のようなconfig情報として記述されている。

## 【0028】

【表2】Config1 (URL情報)

URL01, grp01

URL02, grp02

URL03, grp01, grp02

URL04, grp02, grp03

Cinfig2 (ユーザおよびグループ情報)

grp01, UID=A1\*

grp01, UID=A2001

grp01, UID=A3009

grp02, DESCRIPTION=\*0101

grp03, DESCRIPTION=\*1010

【0029】ここで、“\*”は、ワイルドカードで任意の数の任意の文字がこの位置にあってもよいことを意味する。UIDは、ユーザIDであり、DESCRIPTIONは、ユーザID以外のユーザの属性を表すコードであり、企業内の管理職コード、専門職コード、部門コードなどがその例である。表2のConfig表現をテーブル表示すると次の表3のようになる。

## 【0030】

【表3】

文書	grp01			grp02		grp03
	A1*	A2001	A3009	B0101	C0101	C1010
URL01	○	○	○			
URL02				○	○	
URL03	○	○	○	○	○	
URL04				○	○	○

【0031】表3では、DESCRIPTION=\*0101に該当する属性コードとして、B0101およびC0101があり、DESCRIPTION=\*1010に該当する属性コードとしてC1010があるものと仮定している。このようにアクセス権限は、URL文書単位、グループ単位で設定することができる。

【0032】統合サーバ14は、認証サーバ15からOKメッセージを受け取ると、httpリクエストヘッダを作成してウェブサーバ、今の例では情報提供サーバ17に送られ

る(220)。こうして要求されたコンテンツがブラウザ11に表示される(224)。

【0033】ブロック205で認証Cookieが不正であったり、期限切れであると、認証サーバ15は、NGメッセージを統合サーバ14に送り(208)、統合サーバ14は、NGの理由に応じて再ログインページまたはエラーページをブラウザ11に送る(209)。こうしてブラウザ11に再ログインページまたはエラーページが表示され(21

0)、ユーザはログインを再試行し、またはエラーを訂正することができる。

【0034】統合サーバから認証サーバへのアクセス権限確認処理は、標準的なLDAPプロトコルを用いるが、その他のプロトコルを用いることができることはもちろんである。

【0035】ダイナミックメニュー生成プロセス次に図6を参照してダイナミックメニュー（動的メニュー）の生成プロセスを説明する。ユーザがブラウザ11から統合サーバ14にダイナミックメニューを要求すると

(301)、統合サーバ14は、要求に認証Cookieが付いているかどうかをチェックし(302)、付いていなければログインエラーページをブラウザ11に返(303)、ログインから認証シーケンス(図2)に移る。ダイナミックメニューの要求に認証Cookieが付いていると、統合サーバ14は、メニュー要求メッセージを認証サーバ15に送る(304)。これを受けて認証サーバ15は、アクセス権限をチェックし(305)、このユーザのアクセス権限を示す応答メッセージを統合サーバ14に返す(305)。

【0036】これに回答して統合サーバ14は、メニューテンプレート32を読み込み、認証サーバ15からの応答メッセージで特定されたこのユーザの所属グループに対応するURLを設定ファイル31から読み出してメニューテンプレート32に埋め込む(309)。こうして生成されたダイナミックメニューページがブラウザ11に送られ、ブラウザ11にダイナミックメニューが表示される。この

ダイナミックメニューのメニュー項目にはハイパーリンクが生成されており、ユーザがメニュー項目をクリックすると該当するページへのアクセス要求がブラウザ11から統合サーバ14に送られ、図5に関連して説明したアクセス制御のシーケンスに入る。

【0037】以上にこの発明を具体的な実施の形態を例にとって説明したが、この発明は、このような実施の形態に限定されるものではない。

【図面の簡単な説明】

10 【図1】この発明の一実施例のネットワークシステムの全体的な構成を示すブロック図。

【図2】ダイナミックメニューの生成を行うためのシステムの構成を示すブロック図。

【図3】ブラウザに表示されるダイナミックメニューの例を示す図。ローチャート。

【図4】ユーザ認証プロセスを示すフローチャート。

【図5】アクセス制御のプロセスを示すフローチャート。

20 【図6】ダイナミックメニューの生成プロセスを示すフローチャート。

【符号の説明】

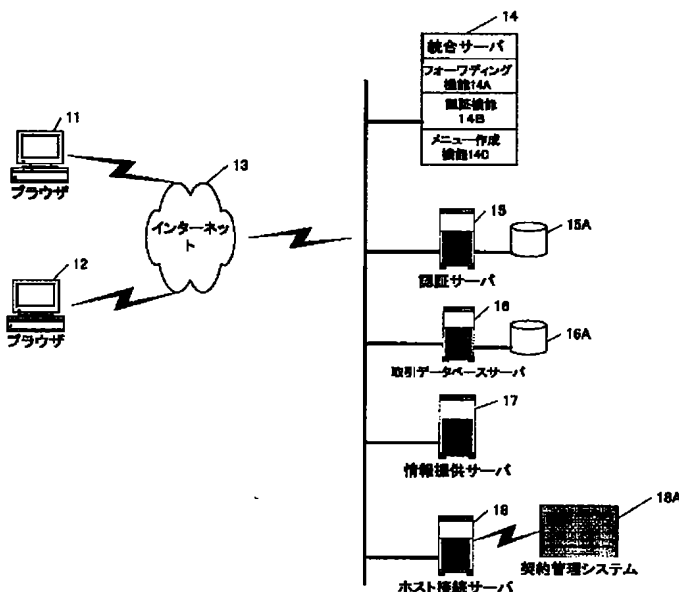
11、12 ブラウザ

14 統合サーバ

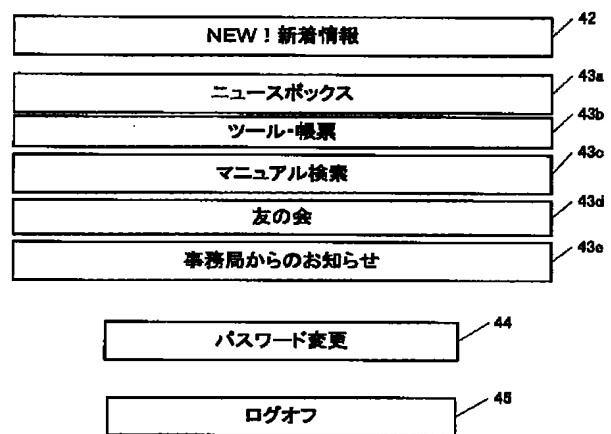
15 認証サーバ

16、17、18 ウェブサーバ

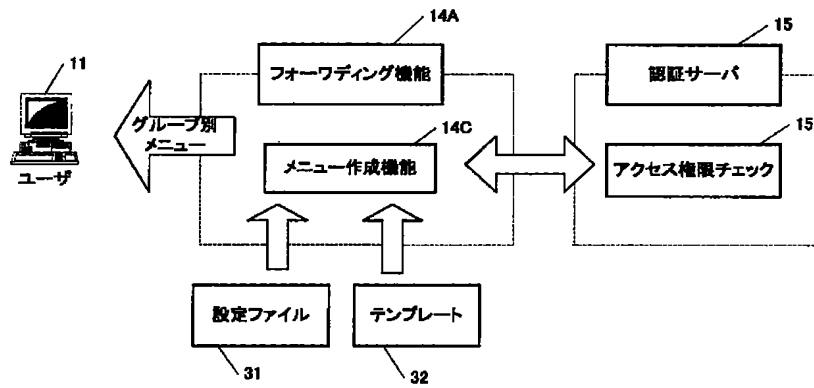
【図1】



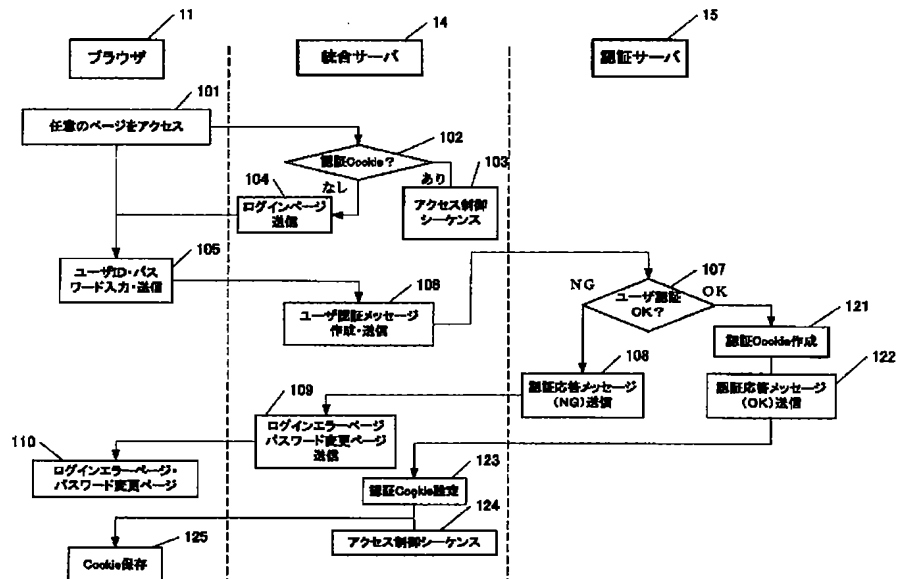
【図3】



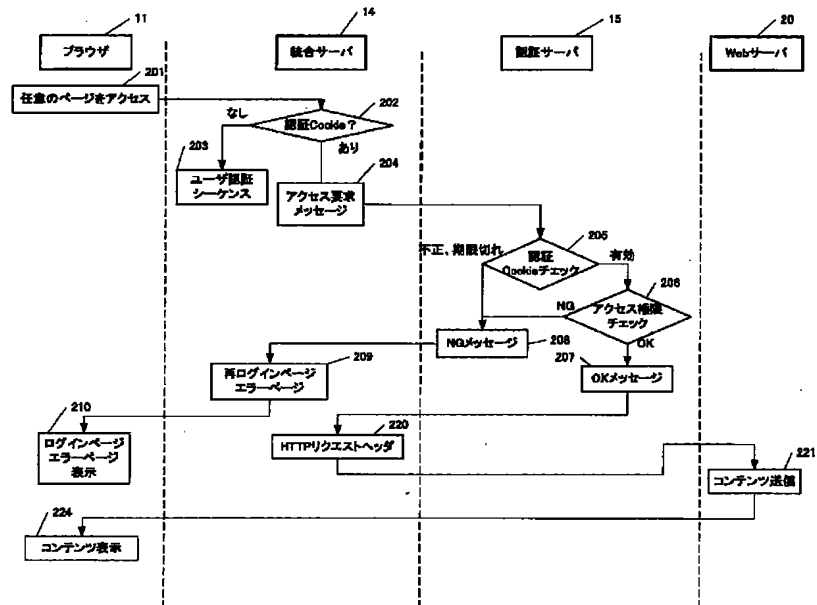
【図2】



【図4】



【図5】



【図6】

